3

[redacted]

WALL STREET JOURNAL
18 October 1985

ARTICLE APPEARED
ON PAGE 31

Study Sheds Light on Vulnerability Of Computers to Electronic Spying

By JOHN J. FIALKA
Staff Reporter of THE WALL STREET JOURNAL

Last fall, a car pulled into a parking lot behind one of the most tightly secured facilities of Holland's Post, Telegraph and Telephone service. A technician inside the car began to work the dials of some simple electronic equipment.

From a faint signal radiating through the back wall of the building, he could tell that a computer terminal was operating inside. Within 15 minutes he had glowing on a television set beside him a duplicate of the image on the terminal's screen.

Fortunately for the Dutch postal authorities, it was an inside job. At work in the car was one of their own electrical engineers, Wim van Eck, 31 years old. His mission was to see whether he could penetrate the system. His tools: a cheap battery-powered TV set, a TV antenna and about $50 worth of basic electronic gear. The results, Mr. van Eck says, "convinced even the most skeptical people in our company of the threat."

Government spy agencies have apparently used similar techniques for years to keep tabs on one another. But Mr. van Eck's was one of the first experiments designed to show that commercial and private users of computer equipment may also have to worry about vulnerability to electronic eavesdropping. And for the first time, the findings of such an experiment will be made public in the U.S.

Guarding Information

The 30-year silence surrounding the matter has been largely the result of a secret National Security Agency program known by the code name Tempest, which was set up to establish standards for safeguarding terminals against high-tech surveillance. Even though Tempest's regulations prohibiting discussion of the problem apply only to the program's members and clients, they have effectively restricted general access to information about it.

This fall, however, the details of Mr. van Eck's experiment will appear in a journal published by the New York-based International Federation for Information Processing, a private group of security-oriented computer specialists. Harold Joseph Highland, a former government cryptographer who is now the journal's editor, says he is printing the van Eck work because the IFIP wants "to show business corporations here that there is a problem and that they may have to think about it."

Computer-security specialists in the U.S. are divided over how vulnerable terminals actually are. Some, including Mr. Highland, believe that the danger of companies' spying on one another's computers is limited in an office complex, where the radiation emitted by a large number of terminals would create an impenetrable electronic fog.

Mr. Highland also doubts that electronic interception is common practice in many businesses. "I don't think Macy's is going over and monitoring Gimbels so that they can plan a sale," he says.

But Belden Menkus, a Middleville, N.J., computer-security consultant who is on the panel that advises the IFIP, is more concerned. He thinks that with off-the-shelf equipment slightly more sophisticated than Mr. van Eck's and costing in the $200 to $400 range, an eavesdropper could go to Wall Street and selectively tune in any desired terminal.

"This may be the age of the passive hacker," says Mr. Menkus, who has heard rumors of industrial espionage using the technique but says he is unable to document any. "Unfortunately," he explains, "nobody wants to come out and admit they've been had in this."

One place an electronic eavesdropper might have more difficulty picking up information from computer terminals is Washington, D.C. Companies say that although federal law permits sales of Tempest-approved equipment in the private sector, almost all of such business comes from the government. For the most part, this is due to NSA efforts over the past six years to persuade federal agencies and defense contractors to buy computer systems built or modified to meet Tempest specifications, which limit the acceptable amount of radiation equipment can give off.

Herbert N. Shearin, who manages the Tempest program at NSA, stated recently in the Journal of Electronic Defense, a trade publication, that 139 companies are currently manufacturing 256 computer products that meet the standards. While this represents only a small fraction of the computer industry overall, interest is increasing.

A Growing Market

Bernard Farkas, president of Systematics General in Sterling, Va., says sales have grown 35% annually over the past few years in his company's division that resells computers it has bought and then modified to meet Tempest standards.

A spokesman for Lowell, Mass.-based Wang Laboratories Inc., reputedly the leading manufacturer of Tempest-approved equipment, says growth in this area has outstripped that of its other markets. And Gene Mitchell, product manager of Delta Data Systems in Trevose, Pa., says 90% of his company's business is now focused on the booming demand for Tempest-approved equipment.

Avner Parnes, chairman of MBI Business Centers, which this year opened the nation's first retail store for Tempest-approved products, in Arlington, Va., estimates that the industry has reached annual sales of $500 million, up from a few thousand dollars five years ago.

To sell such equipment, a company must get on the NSA's Preferred Products List. Until recently, eligibility for this growing roster of endorsed products was set under a kind of honor system.

"You submit to (the NSA) a test plan," explains one Tempest-accredited manufacturer. "They approve the test plan. Then you test to that and submit the results to them. If it meets the specs, you're on the government's list."

But the testing is often left to private agencies, whose work the NSA hasn't always found satisfactory. Mr. Shearin, the Tempest manager, suggested in his statement that there have been cases where cheaper, leak-prone equipment has somehow got onto the program's list.

"Testing organizations," he noted, "are faced with the conflict of ethical considerations versus the monetary benefit of producing a Tempest-accredited product within a set time period." He added that the NSA will reinforce the honor system by doing its own sample testing of various items it has already approved. On this and all other matters regarding Tempest, the NSA declines to respond to questions.

Televisionlike Signals

Government secrecy was a problem for Mr. van Eck, too, when he started his experiment in Holland. The test was designed to help his country's postal agency decide whether it should expand its communications network by placing computer terminals in people's homes. Mr. van Eck says the agency worried about the security of banking by home computer because the government could be liable for losses resulting from a breach of secrecy.

Continued

"We asked the (Dutch) military to give us information on the problem," he recalls. "They wouldn't, so we did research on our own."

Mr. van Eck began by testing 15 brands of home computer systems, including most of the familiar ones sold in the U.S. About 80% of them, he found, emitted a televisionlike signal that could be displayed on a standard TV set once it had been picked up and then restructured by two small electronic devices called oscillators.

The signal, consisting of electromagnetic radiation, emanates both from the terminal's circuitry and from its cathode-ray tube, which shoots the beam of electrons that form the image on the screen, says Mr. van Eck. The trick, he notes, is to capture and interpret that signal.

That's complicated, though, because a standard video-display terminal, like a television, processes input by splitting it into two components: One carries the information; the other is used to synchronize the image, integrating it along vertical and horizontal lines. Mr. van Eck found he could pick up the first of these components but not the second.

Then he learned that he could make sense out of what first appeared to be a clutter of gibberish and static by using oscillators to provide a new synchronization signal. This requires some guesswork, but Mr. van Eck says that if he knows the type of terminal being used he can quickly figure out the synchronization needed.

Two-Mile Range

He says that under ideal conditions he has captured signals from a terminal two miles away. During one experiment conducted for the British Broadcasting Corp., Mr. van Eck says, he parked a van in the basement of an apartment building and managed to read the screen on a terminal in use eight floors above.

The most obvious solution to the problem of eavesdropping, he explains, is to get manufacturers to shield the terminal's internal circuitry with metal and the picture tube with a small mesh screen.

Mr. van Eck says that his research leads him to believe that this method—which U.S. industry sources confirm is the one most commonly used in Tempest-approved products—can be very expensive; because it necessitates practically remaking the equipment, it costs as much as three to six times the original price of the terminal. Mr. van Eck says he is working on a cheaper alternative: a device to scramble or encode the signal in ways that would prevent most eavesdropping.

'The Patience of Job'

Because codes can be broken, however, the government is looking for a more secure defense, according to one man who teaches Tempest techniques to U.S. government officials. "From the government's point of view, you assume that an adversary has the patience of Job," he says.

There are those who remain skeptical of the problem's seriousness. Robert H. Courtney, an engineer who retired in 1981 as director of data security and privacy for International Business Machines Corp., argues that the ease of eavesdropping electronically on computers has been "overstated." He says he is willing to challenge NSA specialists or Mr. van Eck to try to read his terminal from a van outside his office in Port Ewen, N.Y.

Mr. Courtney is aware, though, that the temptation for commercial computer spying exists. "I had a call from the treasurer of a major corporation on (New York City's) Park Avenue," he says. "He'd heard about the problem. There was a major competitor right across the street from his office, and he was convinced they were picking information right off his terminals.

"They were picking it up, all right," Mr. Courtney recalls. "I looked across the street, and there were three pairs of binoculars."